What is claimed is:

1. Method for protecting an exponentiation calculation by means of the Chinese remainder theorem using two prime numbers forming auxiliary modules for calculating auxiliary quantities which may be joined to calculate a modular exponentiation for a module equal to the product of the auxiliary quantities, wherein the exponentiation calculation is performed within a cryptographic algorithm for an encryption of a message, a decryption of a message, a signature generation from a message or a signature verification calculation from a message, the method comprising:

calculating the first auxiliary quantity using the first prime number as the module and using the message;

calculating the second auxiliary quantity using the second prime number as the module and using the message;

combining the first auxiliary quantity and the second auxiliary quantity using a combination algorithm to obtain a result of the exponentiation calculation;

following the combining step, verifying the result of the exponentiation calculation by means of a verifying algorithm, which differs from the combination algorithm, using the first prime number and/or the second prime number, the verifying algorithm providing a predetermined result if the combining step has been performed correctly; and

if the verifying step shows that the verifying algorithm provides a result other than the predetermined result, suppressing an output of the result of the exponentiation calculation.

2. Method as claimed in claim 1, wherein in addition to the result of the exponentiation calculation, the verifying algorithm uses as input data contents of a memory location at

which the first auxiliary quantity, the second auxiliary quantity, the first prime number or the second prime number are stored.

3. Method as claimed in claim 1,

wherein the exponentiation calculation is an RSA encryption, an RSA decryption, an RSA signature calculation or an RSA signature verification calculation.

4. Method as claimed in claim 1,

wherein the combination algorithm is the Garner algorithm.

5. Method as claimed in claim 1,

wherein the verifying algorithm includes a modular reduction of the result of the exponentiation calculation with the first prime number and/or the second prime number as the module.

6. Method as claimed in claim 1,

wherein the first auxiliary quantity is calculated as follows:

$$sp := m^{dp} \bmod p;$$

wherein the second auxiliary quantity is calculated as follows:

$$sq := m^{dq} \bmod q;$$

wherein the combination algorithm is defined as follows:

$$s = sq + \{[(sp-sq)\cdot qinv] \bmod p\} \cdot q; \text{ and}$$

wherein the verification algorithm is defined as follows:

$$s \bmod p = sp; \text{ and/or}$$

s mod q = sq; and

wherein the predetermined result is an equality condition in the verification algorithm.

7. Method as claimed in claim 1, further comprising:

after the step of combining the first auxiliary quantity and the second auxiliary quantity, verifying whether any input data for the exponentiation calculation have been changed, and, if this is so, suppressing the result of the exponentiation calculation.

8. Method as claimed in claim 7, wherein a random number is used for verifying auxiliary exponents.

9. Method as claimed in claim 7, wherein a prime number is used as input data for verifying the first prime number and the second prime number.

10. Method as claimed in claim 9, wherein the prime number has a number of digits which is smaller than the number of digits of the first prime number and of the second prime number.

11. Apparatus for protecting an exponentiation calculation by means of the Chinese remainder theorem using two prime numbers forming auxiliary modules for a calculation of auxiliary quantities which may be joined to calculate a modular exponentiation for a module which is equal to the product of the auxiliary quantities, wherein the exponentiation calculation is performed within a cryptographic algorithm for an encryption of a message, a decryption of a message, a signature generation from a message or a signature verification calculation from a message, the apparatus comprising:

a calculator calculating the first auxiliary quantity using the first prime number as the module and using the message;

a calculator for calculating the second auxiliary quantity using the second prime number as the module and using the message;

a combiner for combining the first auxiliary quantity and the second auxiliary quantity using a combination algorithm to obtain a result of the exponentiation calculation;

a verifier for verifying the result of the exponentiation calculation by means of a verifying algorithm, which differs from the combination algorithm, using the first prime number and/or the second prime number, the verifying algorithm providing a predetermined result if the means for combining has provided a correct result; and

a suppressor for suppressing an output of the result of the exponentiation calculation if the means for verifying indicates that the verifying algorithm provides a result other than the predetermined result.